CLAIMS

1. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on an elliptic curve in the elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of said scalar-multiplied point; and a step of recovering a complete coordinate from the partial information of said scalar-multiplied point.

2. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on an elliptic curve in the elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of said scalar-multiplied point; and a step of recovering a complete coordinate in affine coordinates from the partial information of said scalar-multiplied point.

3. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on an elliptic curve in the elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of

said scalar-multiplied point; and a step of recovering a complete coordinate in projective coordinates from the partial information of said scalar-multiplied point.

4. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Montgomery-form elliptic curve in the Montgomery-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of said scalar-multiplied point; and a step of recovering a complete coordinate from the partial information of said scalar-multiplied point.

5. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Weierstrass-form elliptic curve in the Weierstrass-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of said scalar-multiplied point; and a step of recovering a complete coordinate from the partial information of said scalar-multiplied point.

6. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Montgomery-form elliptic curve in the Montgomery-form elliptic curve defined on a finite

field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of said scalar-multiplied point; and a step of giving X-coordinate and Z-coordinate of said scalar-multiplied point given as the partial information of said scalar-multiplied point in projective coordinates and X-coordinate and Z-coordinate of a point obtained by adding said scalar-multiplied point and the point on said Montgomery-form elliptic curve in the projective coordinates, and recovering a complete coordinate in affine coordinates.

7. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Montgomery-form elliptic curve in the Montgomery-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of said scalar-multiplied point; and a step of giving X-coordinate and Z-coordinate of said scalar-multiplied point given as the partial information of said scalar-multiplied point in projective coordinates and X-coordinate and Z-coordinate of a point obtained by adding said scalar-multiplied point and the point on said Montgomery-form elliptic curve in the projective coordinates, and recovering a complete coordinate in the projective coordinates.

8. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Montgomery-form elliptic curve in the Montgomery-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of said scalar-multiplied point; and a step of giving X-coordinate and Z-coordinate of said scalar-multiplied point given as the partial information of said scalar-multiplied point in projective coordinates, X-coordinate and Z-coordinate of a point obtained by adding said scalar-multiplied point and the point on said Montgomery-form elliptic curve in the projective coordinates, and X-coordinate and Z-coordinate of a point obtained by subtracting said scalar-multiplied point and the point on said Montgomery-form elliptic curve in the projective coordinates, and recovering a complete coordinate in affine coordinates.

9. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Montgomery-form elliptic curve in the Montgomery-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of said scalar-multiplied point; and a step of giving X-coordinate and Z-coordinate of said scalar-multiplied

point given as the partial information of said scalar-multiplied point in projective coordinates, X-coordinate and Z-coordinate of a point obtained by adding said scalar-multiplied point and the point on said Montgomery-form elliptic curve in the projective coordinates, and X-coordinate and Z-coordinate of a point obtained by subtracting said scalar-multiplied point and the point on said Montgomery-form elliptic curve in the projective coordinates, and recovering a complete coordinate in the projective coordinates.

10. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Montgomery-form elliptic curve in the Montgomery-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of said scalar-multiplied point; and a step of giving x-coordinate of the scalar-multiplied point given as the partial information of said scalar-multiplied point in affine coordinates, x-coordinate of a point obtained by adding said scalar-multiplied point and the point on said Montgomery-form elliptic curve in the affine coordinates, and x-coordinate of a point obtained by subtracting said scalar-multiplied point and the point on said Montgomery-form elliptic curve in the affine coordinates, and recovering a complete coordinate in the affine coordinates.

11. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Weierstrass-form elliptic curve in the Weierstrass-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of the scalar-multiplied point; and a step of giving X-coordinate and Z-coordinate of the scalar-multiplied point given as the partial information of said scalar-multiplied point in projective coordinates, X-coordinate and Z-coordinate of a point obtained by adding said scalar-multiplied point and the point on said Weierstrass-form elliptic curve in the projective coordinates, and X-coordinate and Z-coordinate of a point obtained by subtracting said scalar-multiplied point and the point on said Weierstrass-form elliptic curve in the projective coordinates, and recovering a complete coordinate in affine coordinates.

12. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Weierstrass-form elliptic curve in the Weierstrass-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of the scalar-multiplied point; and a step of giving X-coordinate and Z-coordinate of said scalar-multiplied

point given as the partial information of said scalar-multiplied point in projective coordinates, X-coordinate and Z-coordinate of a point obtained by adding said scalar-multiplied point and the point on said Weierstrass-form elliptic curve in the projective coordinates, and X-coordinate and Z-coordinate of a point obtained by subtracting said scalar-multiplied point and the point on said Weierstrass-form elliptic curve in the projective coordinates, and recovering a complete coordinate in the projective coordinates.

13. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Weierstrass-form elliptic curve in the Weierstrass-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of calculating partial information of said scalar-multiplied point; and a step of giving x-coordinate of said scalar-multiplied point given as the partial information of said scalar-multiplied point in affine coordinates, x-coordinate of a point obtained by adding said scalar-multiplied point and the point on said Weierstrass-form elliptic curve in the affine coordinates, and x-coordinate of a point obtained by subtracting said scalar-multiplied point and the point on said Weierstrass-form elliptic curve in the affine coordinates, and recovering a complete coordinate in the affine coordinates.

14. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Weierstrass-form elliptic curve in the Weierstrass-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of transforming said Weierstrass-form elliptic curve to a Montgomery-form elliptic curve; a step of calculating partial information of the scalar-multiplied point in the Montgomery-form elliptic curve; and a step of recovering a complete coordinate in the Weierstrass-form elliptic curve from the partial information of the scalar-multiplied point in said Montgomery-form elliptic curve.

15. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Weierstrass-form elliptic curve in the Weierstrass-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of transforming said Weierstrass-form elliptic curve to a Montgomery-form elliptic curve; a step of calculating partial information of the scalar-multiplied point in said Montgomery-form elliptic curve; a step of recovering a complete coordinate in said Montgomery-form elliptic curve from the partial information of the scalar-multiplied point in the Montgomery-form elliptic curve; and a step of

calculating the scalar-multiplied point in the Weierstrass-form elliptic curve from the scalar-multiplied point in which the complete coordinate is recovered in said Montgomery-form elliptic curve.

16. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Weierstrass-form elliptic curve in the Weierstrass-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of transforming said Weierstrass-form elliptic curve to a Montgomery-form elliptic curve; a step of calculating partial information of the scalar-multiplied point in said Montgomery-form elliptic curve; and a step of giving X-coordinate and Z-coordinate of the scalar-multiplied point given as the partial information of the scalar-multiplied point in the Montgomery-form elliptic curve in projective coordinates in the Montgomery-form elliptic curve, and X-coordinate and Z-coordinate of a point obtained by adding said scalar-multiplied point and the point on the Montgomery-form elliptic curve in the projective coordinates, and recovering a complete coordinate in affine coordinates in the Weierstrass-form elliptic curve.

17. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Weierstrass-form elliptic curve in the

Weierstrass-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of transforming said Weierstrass-form elliptic curve to a Montgomery-form elliptic curve; a step of calculating partial information of the scalar-multiplied point in said Montgomery-form elliptic curve; and a step of giving X-coordinate and Z-coordinate of the scalar-multiplied point given as the partial information of the scalar-multiplied point in the Montgomery-form elliptic curve in projective coordinates in the Montgomery-form elliptic curve, and X-coordinate and Z-coordinate of a point obtained by adding said scalar-multiplied point and the point on the Montgomery-form elliptic curve in the projective coordinates, and recovering a complete coordinate in the projective coordinates in the Weierstrass-form elliptic curve.

18. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Weierstrass-form elliptic curve in the Weierstrass-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of transforming said Weierstrass-form elliptic curve to a Montgomery-form elliptic curve; a step of calculating partial information of the scalar-multiplied point in said Montgomery-form elliptic

curve; and a step of giving X-coordinate and Z-coordinate of the scalar-multiplied point given as the partial information of the scalar-multiplied point in the Montgomery-form elliptic curve in projective coordinates in the Montgomery-form elliptic curve, X-coordinate and Z-coordinate of a point obtained by adding said scalar-multiplied point and the point on the Montgomery-form elliptic curve in the projective coordinates, and X-coordinate and Z-coordinate of a point obtained by subtracting said scalar-multiplied point and the point on the Montgomery-form elliptic curve in the projective coordinates, and recovering a complete coordinate in affine coordinates in the Weierstrass-form elliptic curve.

19. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Weierstrass-form elliptic curve in the Weierstrass-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of transforming said Weierstrass-form elliptic curve to a Montgomery-form elliptic curve; a step of calculating partial information of the scalar-multiplied point in said Montgomery-form elliptic curve; and a step of giving X-coordinate and Z-coordinate of the scalar-multiplied point given as the partial information of the scalar-multiplied point in the Montgomery-form elliptic curve in projective

coordinates in the Montgomery-form elliptic curve, X-coordinate and Z-coordinate of a point obtained by adding said scalar-multiplied point and the point on the Montgomery-form elliptic curve in the projective coordinates, and X-coordinate and Z-coordinate of a point obtained by subtracting said scalar-multiplied point and the point on the Montgomery-form elliptic curve in the projective coordinates, and recovering a complete coordinate in the projective coordinates in the Weierstrass-form elliptic curve.

20. A scalar multiplication method for calculating a scalar-multiplied point from a scalar value and a point on a Weierstrass-form elliptic curve in the Weierstrass-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the method comprising:

a step of transforming said Weierstrass-form elliptic curve to a Montgomery-form elliptic curve; a step of calculating partial information of the scalar-multiplied point in said Montgomery-form elliptic curve; and a step of giving x-coordinate of the scalar-multiplied point given as the partial information of the scalar-multiplied point in said Montgomery-form elliptic curve in affine coordinates in the Montgomery-form elliptic curve, x-coordinate of a point obtained by adding said scalar-multiplied point and the point on the Montgomery-form elliptic curve in the affine coordinates, and x-coordinate of a point obtained by

subtracting said scalar-multiplied point and the point on the Montgomery-form elliptic curve in the affine coordinates, and recovering a complete coordinate in the affine coordinates in the Weierstrass-form elliptic curve.

21. A data generation method for generating second data from first data, comprising a step of using the scalar multiplication method according to any one of claims 1 to 20 to calculate scalar multiplication.

22. A signature generation method for generating signature data from data, comprising a step of using the scalar multiplication method according to any one of claims 1 to 20 to calculate scalar multiplication.

23. A decryption method for generating decrypted data from encrypted data, comprising a step of using the scalar multiplication method according to any one of claims 1 to 20 to calculate scalar multiplication.

24. A scalar multiplication apparatus which calculates a scalar-multiplied point from a scalar value and a point on an elliptic curve in the elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the unit comprising:

a fast scalar multiplication unit which calculates partial information of said scalar-multiplied point; and a coordinate recovering unit which recovers a complete coordinate from the partial information of said scalar-multiplied point,

wherein said scalar multiplication apparatus calculates the partial information of the scalar-multiplied point by the fast scalar multiplication unit, recovers the complete coordinate from the partial information of the scalar-multiplied point by the coordinate recovering unit, and calculates the scalar-multiplied point.

25. A scalar multiplication apparatus for calculating a scalar-multiplied point from a scalar value and a point on a Weierstrass-form elliptic curve in the elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, the apparatus comprising:

an elliptic curve transform unit which transforms said Weierstrass-form elliptic curve to a Montgomery-form elliptic curve; a fast scalar multiplication unit which calculates partial information of said scalar-multiplied point; a coordinate recovering unit which recovers a complete coordinate from the partial information from said scalar-multiplied point; and an elliptic curve inverse transform unit which transforms the Montgomery-form elliptic curve to the Weierstrass-form elliptic curve,

wherein said scalar multiplication apparatus transforms said Weierstrass-form elliptic curve to the Montgomery-form elliptic curve by the elliptic curve transform unit, calculates the partial information of the scalar-multiplied point in the Montgomery-form

elliptic curve by the fast scalar multiplication unit, recovers a complete coordinate in the Montgomery-form elliptic curve from the partial information of the scalar-multiplied point in said Montgomery-form elliptic curve by the coordinate recovering unit, calculates the scalar-multiplied point in the Weierstrass-form elliptic curve from the scalar-multiplied point with the complete coordinate recovered in the Montgomery-form elliptic curve by the elliptic curve by the elliptic curve inverse transform unit.

26. A storage medium wherein program relating to the scalar multiplication method according to any one of claims 1 to 20 is stored.

27. A coordinate recovering method for recovering a complete coordinate from a point on an elliptic curve given by an incomplete coordinate in the elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, said method comprising:

a step of calculating a coordinate of the point having said incomplete coordinate from the point having said incomplete coordinate and a point obtained by addition and subtraction of the point having said incomplete coordinate and a point having the complete coordinate.

28. A coordinate recovering method for recovering a complete coordinate from a point on an elliptic curve given by an incomplete coordinate in the elliptic curve

defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, said method comprising:

a step of calculating a point obtained by subtraction of the point having said incomplete coordinate and a point having the complete coordinate from the point having said incomplete coordinate and a point obtained by addition of the point having said incomplete coordinate and the point having the complete coordinate; and a step of calculating the coordinate of the point having said incomplete coordinate.

29. A coordinate recovering method for recovering a complete coordinate in a Weierstrass-form elliptic curve from a point on a Montgomery-form elliptic curve given by an incomplete coordinate in the Montgomery-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, said method comprising:

a step of calculating a coordinate of the point having the incomplete coordinate in said Montgomery-form elliptic curve from the point having the incomplete coordinate in said Montgomery-form elliptic curve and a point obtained by addition and subtraction of the point having the incomplete coordinate in said Montgomery-form elliptic curve and a point having the complete coordinate; and a step of transforming the point of the Montgomery-form elliptic curve having said complete coordinate calculated to a

point of the Weierstrass-form elliptic curve.

30. A coordinate recovering method for recovering a complete coordinate in a Weierstrass-form elliptic curve from a point on a Montgomery-form elliptic curve given by an incomplete coordinate in the Montgomery-form elliptic curve defined on a finite field with characteristics of 5 or more in an elliptic curve cryptosystem, said method comprising:

a step of calculating a point obtained by subtraction of a point having the incomplete coordinate in said Montgomery-form elliptic curve and a point having a complete coordinate from the point having the incomplete coordinate in said Montgomery-form elliptic curve and a point by addition of the point having the incomplete coordinate in said Montgomery-form elliptic curve and the point having the complete coordinate; a step of calculating a coordinate of the point having the incomplete coordinate in said Montgomery-form elliptic curve; and a step of transforming the point of the Montgomery-form elliptic curve having said complete coordinate calculated to a point of the Weierstrass-form elliptic curve.